1 Ekwan E. Rhow - State Bar No. 174604
       erhow@birdmarella.com
2 Marc E. Masters - State Bar No. 208375
       mmasters@birdmarella.com
3 BIRD, MARELLA, RHOW,
   LINCENBERG, DROOKS, & NESSIM, LLP
4 1875 Century Park East, 23rd Floor
   Los Angeles, California 90067-2561
5 Telephone: (310) 201-2100
   Facsimile: (310) 201-2110
6
   Jonathan M. Rotter - State Bar No. 234137
7 jrotter@glancylaw.com
   David J. Stone - State Bar No. 208961
8 dstone@glancylaw.com
   GLANCY PRONGAY & MURRAY LLP
9 1925 Century Park East, Suite 2100
   Los Angeles, California 90067-2561
10 Telephone: (310) 201-9150
   Email: info@glancylaw.com
11
   Korey A. Nelson (admitted pro hac)
12 knelson@burnscharest.com
   Amanda K. Klevorn (admitted pro hac)
13 aklevorn@burnscharest.com
   Claire Bosarge Curwick (admitted pro hac)
14 ccurwick@burnscharest.com
   Logan B. Fontenot (admitted pro hac)
15 lfontenot@burnscharest.com
   BURNS CHAREST LLP
16 365 Canal Street, Suite 1170
   New Orleans, LA 70130
17 Telephone: (504) 799-2845

18 Attorneys for Plaintiffs

19   UNITED STATES DISTRICT COURT
            NORTHERN DISTRICT OF CALIFORNIA
20   SAN FRANCISCO DIVISION

21 GRACE LAU, CHRISTOPHER   CASE NO. 3:22-cv-08981-RFL
   KARWOWSKI, MELODY KLEIN,
22 MICHAEL MCBRIDE, and AIMEN HALIM,   **DECLARATION OF ATIF HASHMI IN**
   individual and on behalf of all others similarly   **SUPPORT OF PLAINTIFFS' MOTION**
23 situated;   **TO COMPEL COMPLIANCE WITH**
                                             SUBPOENAS PURSUANT TO FEDERAL
24   Plaintiffs,   **RULE OF CIVIL PROCEDURE 45**

25   vs.

26 GEN DIGITAL INC. a corporation, and
   JUMPSHOT INC., a corporation,
27
             Defendants.
28

3979997.10

1

DECLARATION OF ATIF HASHMI

2   I, Atif Hashmi, declare as follows:

3   1.   I am the President and Chief Scientist of Bitwise Forensics Research, Inc.,

4   which provides engineering consulting services. My clients have included large computer

5   and technology companies as well as smaller companies and startups. I am fully familiar

6   with the facts contained herein based upon my personal knowledge, analysis, and upon

7   information provided by Plaintiffs' Counsel, and if called as a witness, could and would

8   testify competently thereto. I submit this declaration at the request of Plaintiffs' Counsel

9   in connection with the above-captioned action (the "Action").

10   2.   I hold a B.S. in Computer Engineering from Lahore University of

11   Management Sciences ("LUMS") in Pakistan. I also hold an M.S. and Ph.D. in Electrical

12   Engineering from the University of Wisconsin in Madison, Wisconsin. My educational

13   training and research have been focused on software engineering, computer architecture,

14   machine learning, operating systems, and design and development of hardware circuits and

15   software for computing systems. I have more than 20 years of experience in software

16   design and development for distributed systems, embedded devices, server-client based

17   systems, mobile platforms, operating systems, neural networks, and machine learning

18   based platforms. I have studied and developed software using programming languages

19   including C, C++, Java, Python, JavaScript, Embedded C, Assembly Language, PHP, and

20   others.

21   3.   I have published research papers related to machine learning, artificial

22   intelligence, computer hardware, and software in peer-reviewed computer science and

23   electrical engineering conferences. Several of these publications have received best

24   research paper awards. I have been an invited speaker at venues including academic

25   conferences and technology companies. I have been an expert due-diligence panelist for

26   the National Science Foundation to evaluate proposal submitted to NSF in the areas of

27   sensor-based systems and machine learning. I am a named inventor on patents and patent

28   applications for neural network software and hardware for processing sensory data. A

2

1 complete list of patents and patent applications on which I am a named inventor is

2 included in my CV, attached hereto as **Exhibit A**.

3   4.   Over the years, I have consulted in over 100 legal matters involving software

4 copyright infringement, privacy, trade secret theft, source code quality, and patent

5 infringement. I have given testimony as an expert and submitted reports in which I offered

6 opinions regarding my technical analysis. As a technical expert, I have reviewed thousands

7 of lines of source code developed in several programming and hardware descriptive

8 languages including C/C++, Java, JavaScript, Ruby, SQL, and Verilog-HDL. Additional

9 details about specific cases can be found in my CV. *See* Ex. A.

10   5.   I am being compensated at a rate of $700 per hour in connection with this

11 declaration. My findings are still preliminary as my analysis related to this matter is

12 ongoing.

13   6.   I performed a detailed analysis and review of network traffic comprising the

14 cookies exchanged between a device that has the Avast Online Security and Privacy

15 ("AOSP") browser extension plugin installed ("AOSP Client Device"), Avast's servers,

16 and various websites accessed using the Microsoft Edge and Google Chrome internet

17 browser. This analysis revealed that, after visiting https://www.avast.com, whether as

18 directed during the AOSP installation process or otherwise, when an AOSP Client Device

19 visits a website and thereby sends a request to the server hosting that website, the AOSP

20 browser extension plugin intercepts that request and sends the URL of the website and

21 cookie identifiers (discussed below) to the Avast's servers via the urlite.ff.avast.com

22 subdomain. By analyzing the source code that runs on Avast's servers, I can determine

23 whether the data sent by the AOSP browser extension plugin, including the URL and

24 cookie identifiers, is accessed by Avast servers, and what (if anything) Avast's servers do

25 with that data.

26   7.   Based on my analysis and review of the network traffic between the AOSP

27 Client Device and Avast's servers, I determined that the AOSP Client Device, at various

28 times sent the following cookies from third-party companies bearing the corresponding

cookie identifiers to Avast's servers: (i) Adobe Inc.: AMCV_, AMCVS_, and s_nr, ;[1] (ii)

Alphabet Inc.: _ga, _gcl_au, and _gid;[2] (iii) META Platforms Inc.: _fbp;[3] (iv) Microsoft

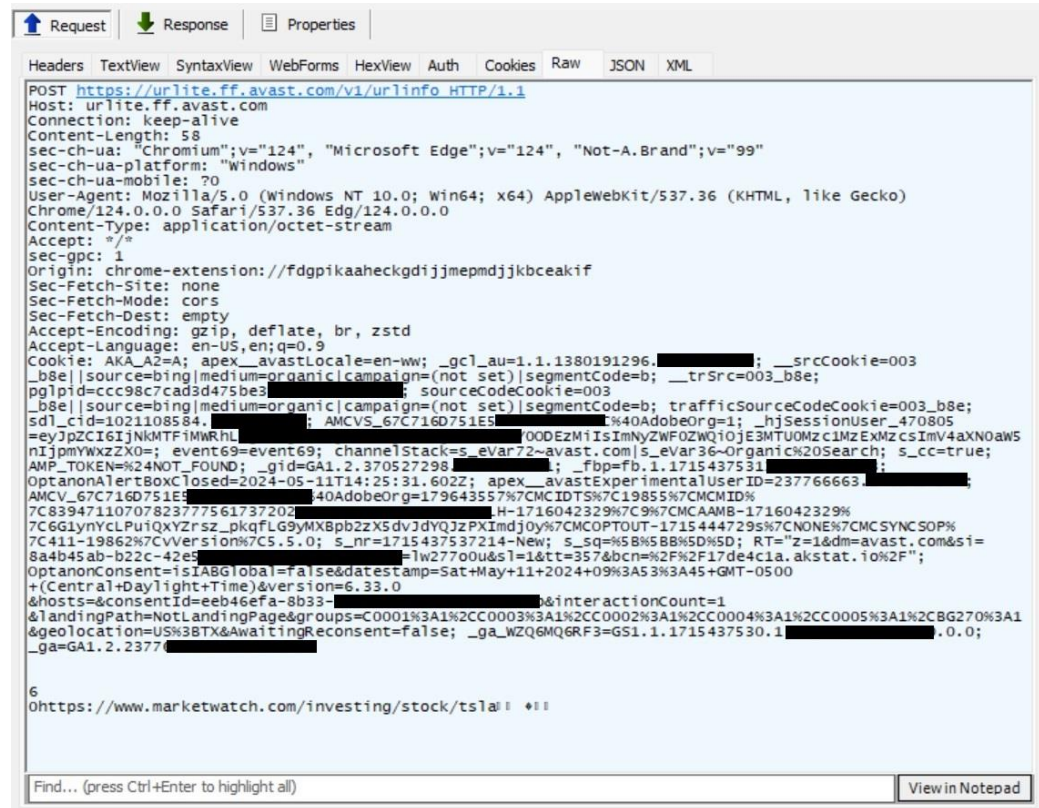Corporation: _uetvid;[4] and (v) Reddit, Inc.: _rdt_uuid.[5] An example of data sent by an

Figure 1: Data including URL and Cookie Identifiers sent by the AOSP Client Device to Avast's servers.

---

[1] *See Cookies and the Experience Cloud Identity Service*, Adobe Experience League, (Aug. 23, 2024), https://experienceleague.adobe.com/en/docs/id-service/using/intro/cookies; *see also Adobe plug-in: getNewRepeat*, Adobe Experience League, (Aug. 23, 2024), https://experienceleague.adobe.com/en/docs/analytics/implementation/vars/plugins/getnew repeat.

[2] *See How Google Uses Cookies*, Google Privacy & Terms, (Aug. 23, 2024), https://policies.google.com/technologies/cookies?hl=en-US; *see also Our advertising and measurement cookies*, Google, (Aug. 23, 2024), https://business.safety.google/adscookies/.

[3] *See ClickID and the fbp and fbc Parameters*, Meta for Developers, (Aug. 23, 2024), https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/fbp-and-fbc/.

[4] *See FAQ: Universal Event Tracking*, Microsoft Ads Help, (Aug. 26, 2024), https://help.ads.microsoft.com/apex/index/3/en/53056/.

[5] *See Cookie Policy*, Super Metrics Cookie Policy, (Aug. 26, 2024), https://supermetrics.com/cookie-policy; Also see *LinkedIn Cookie Table*, LinkedIn Legal, (Aug. 26, 2024), https://www.linkedin.com/legal/l/cookie-table.

1 AOSP Client Device to Avast's servers is shown in Figure 1.

2   8.   Cookies and corresponding cookie identifiers are appended to the

3 transmission to Avast's servers via the urlite.ff.avast.com subdomain, because the cookies

4 set by avast.com at the outset of the process are configured in a way to allow those cookies

5 to be sent to Avast's servers via the urlite.ff.avast.com subdomain. More specifically: a

6 server can send the Set-Cookie header to set up or install a cookie on a user's device. That

7 is what Avast's servers do when the AOSP Client Device accesses https://www.avast.com.

8 Within the Set-Cookie headers, the Domain and Path attributes define the scope of a

9 cookie, *i.e.*, what servers the cookies are sent to. If the Set-Cookie header does not

10 specify/include a Domain attribute, the cookies are available on the server that sets it but

11 not on its subdomains.[6] Based on my testing in May 2024, as shown in Figure 2,

12 Defendant specifically set the Domain attribute in a way that causes the cookies to be sent

13 to the Avast's servers via the urlite.ff.avast.com subdomain. Defendant could have

14 configured the Set-Cookie headers such that cookies and corresponding cookie identifiers

Figure 2: Response from Avast's servers showing that the domain element of Set-Cookie header is set to avast.com (May 2024).

24 are not sent to Avast's servers via the urlite.ff.avast.com subdomain. In other words,

25 Defendant could have configured the Set-Cookie header such that AOSP would not have

26 sent cookies back to Defendant along with users' browsing data.

27

[6] *See Using HTTP cookies*, MDN Web Docs, (Aug. 23, 2024),
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies.

9.   A comparison of the responses from Avast's servers returned during my analysis conducted in May 2024 with responses from Avast's servers on August 23, 2024, reveals that this configuration is not only possible, but is, in fact, now employed by Avast. In May 2024, the responses from Avast's servers confirmed that Defendant affirmatively set the Domain attribute to "avast.com," causing the cookies, along with an AOSP Client Device's browsing data, to be sent to Avast's servers. In other words, any subdomain of avast.com, including urlite.ff.avast.com, would send cookie and browsing data to Avast's servers.[7] Now, it appears that Defendants have modified their system to remove this functionality.

10.   As shown in Figure 3, as of August 23, 2024, Defendant has reconfigured the Set-Cookie header to remove the Domain attribute parameter, meaning that Avast may still collect cookie data, but the cookie data is no longer sent to Avast's servers via Avast's subdomains, including urlite.ff.avast.com. Contrary to Defendant's assertion that the browser, not Avast, is responsible for embedding the cookies in the network traffic, this comparison confirms that Defendant always had the ability to exclude browsing data from urlite.ff.avast.com from the network traffic to Avast's servers.

```
HTTP/1.1 302 Moved Temporarily
Server: AkamaiGHost
Content-Length: 0
Location: https://www.avast.com/en-us/index
Date: Fri, 23 Aug 2024 17:35:00 GMT
Connection: keep-alive
Set-Cookie: avastComLocale=en-us; expires=Mon, 31-Dec-2038 23:59:59 GMT; path=/
Set-Cookie: bandwidth=5000
Server-Timing: cdn-cache; desc=HIT
Server-Timing: edge; dur=1
Server-Timing: ak_p; desc="1724434500679_399076071_578608095_46_7668_12_14_-";dur=1
```

Figure 3: Response from Avast's servers showing that the domain element of Set-Cookie header is not set (August 2024).

11.   Cookies of the type installed by Avast's servers (e.g., Google cookies, Meta cookies, etc.) when the AOSP Client Device accesses https://www.avast.com can be sent together with browsing data to the corresponding third parties for analytics and other purposes.[8] Along with the analysis of source code that runs on Avast's servers,

---

[7] This is also confirmed by the Defendant's August 16, 2024, correspondence to Plaintiffs, attached hereto as **Exhibit B.**

[8] For example, *see Client-side tagging vs. server-side tagging*, Google Tag Manager Help,

1 determining whether Avast's servers after receiving data from an AOSP Client Device

2 transmits that data to third parties requires review of the data transmitted to the identified

3 third-party servers by Avast's servers, and review of the data received by the third-party

4 servers from Avast's servers.

5   12.   I have reviewed the arguments raised by Defendant in their August 16 letter

6 and the underlying evidence provided.[9] The excerpts of source code provided by the

7 Defendant are insufficient to determine whether and how Avast uses the subject cookies.

8 Moreover, the evidence cited in support of the Defendant's August 16 letter is incomplete

9 or otherwise does not provide a full picture of Avast's server activity as it relates to

10 collection and storage of users' data and associated cookies.

11   13.   This declaration is based on information currently available to me. To the

12 extent that additional information becomes available, I reserve the right to continue my

13 investigation and study, and thus may expand or modify my declaration as my

14 investigation and study continues. I also reserve the right to supplement my declaration in

15 response to any additional information that becomes available to me, any matters raised by

16

17 (Aug. 23, 2024), https://support.google.com/tagmanager/answer/13387731?hl=en. *See also What is server-side tagging?*, Google Tags (Aug. 23, 2024),

18 https://developers.google.com/tag-platform/tag-manager/server-side; *Manual Setup Guide*, Google Tags (Aug. 23, 2024), https://developers.google.com/tag-platform/tag-

19 manager/server-side/manual-setup-guide; *Google Analytics 4: Reuse event settings in Google Tag Manager*, Google Tag Manager Help (Aug. 23, 2024),

20 https://support.google.com/tagmanager/answer/13438771; *Send data to server-side Tag Manager*, Google Tags (Aug. 23, 2024), https://developers.google.com/tag-platform/tag-

21 manager/server-side/send-data?option=GTM#server-to-server_apps; S*et Up Conversions API for Server-Side Tagging in Google Tag Manager*, Meta Business Help Center (Aug.

22 23, 2024), https://www.facebook.com/business/help/702509907046774; *Conversions API for Server-Side Google Tag Manager (GTM)*, Meta for Developers (Aug. 23, 2024),

23

24 https://developers.facebook.com/docs/marketing-api/conversions-api/guides/gtm-server-side/; *Facebook Server Side Tracking*, Taggrs (Aug. 23, 2024),

25 https://taggrs.io/en/facebook-server-side-tracking/; *Conversions API*, Meta for Developers (Aug. 23, 2024), https://developers.facebook.com/docs/marketing-api/conversions-api/;

26 *Using the API*, Meta for Developers (Aug. 23, 2024),

27 https://developers.facebook.com/docs/marketing-api/conversions-api/using-the-api.

[9] See the Defendant's August 16, 2024, correspondence to Plaintiffs, attached hereto as

28 **Exhibit B.**

1 Defendant and/or opinions rendered by Defendant's experts, or in light of any relevant

2 orders from the Court.

3

4   I declare under penalty of perjury under the laws of the State of California that the

5 foregoing is true and correct.

6

7   Executed August 26, 2024, at Prosper, Texas.

8

9   _____

10   Atif Hashmi

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

8

EXHIBIT A

ATIF HASHMI

Dallas, TX

PROFESSIONAL ACCOMPLISHMENTS

- Expert in computer software and hardware with 15+ years of professional experience
- Inventor with multiple issued and pending patents
- Publications in top-tier computer software/hardware peer reviewed conferences and journals
- Speaker at prestigious venues including computer software and hardware conferences and workshops
- Expert due-diligence panelist/advisor for National Science Foundation

EMPLOYMENT

- **President and Chief Scientist**   **2016 – present**
  Bitwise Forensics Research, Inc.
  - Provide engineering research and design services
  - Provide intellectual property and litigation consulting
  - Perform software source code analysis for copyright infringement and trade secret cases
  - Perform patent infringement and invalidity analysis

- **Founder and Chief Technology Officer**   **2013 – 2017**
  Thalchemy Corporation
  - Develop neuromorphic hardware substrate and software algorithms to enable ultralow power analysis of sensory data in real time
  - Develop software development kit to interface the continuous sensing hardware with general purpose computational processing units
  - Optimize "always-on" sensing algorithms to run on ARM M0 and M4 based sensor hubs for low memory and small memory footprint
  - Develop motion and audio sensing algorithms to enable context aware sensing
  - Principal Investigator for NSF SBIR Phase I/II grants awarded to Thalchemy Corporation
  - Fund raising (Angels, VCs, SBIR, STTR, etc.)

- **Post-Doctoral Associate**   **2011 – 2012**
  Wisconsin Psychiatric Research Institute
  - Worked on the IBM/DARPA SyNAPSE project
  - Developed detailed software models of different regions of the mammalian brain
  - Developed software tools in C/C++ and Java to automate the deployment of neural networks
  - Designed functional templates for various regions of the mammalian visual cortex
  - Developed placement schemes to optimize the overall interconnect dynamic power
  - Developed placement schemes for complex biological networks to optimize the overall interconnect dynamic power

- **Graduate Intern (Technical)**   **2006 –2007**
  Intel Corporation

1

- Worked on Intel's graphic processor tool-chain including the functional simulation model and the cycle accurate simulator for Intel's graphic processing core
- Analyzed various 3D graphics workloads and conducted performance studies using hardware counters and simulation tools on Intel's next generation graphics processing unit
- Designed experiments to identify performance bottlenecks within the GPU pipeline

EDUCATION

- **Ph.D. in Electrical Engineering,** *University of Wisconsin, Madison*   **2011**
  Thesis: Cortical Columns: A Non von Neumann Computational Abstraction
  Research Focus: Brain inspired computing, hardware/software modeling of neural systems

- **M.S. in Electrical Engineering,** *University of Wisconsin, Madison*   **2007**
  Thesis: Accelerating Search and Recognition with a TCAM Functional Unit
  Research Focus: Computer Architecture
  Minor Area: Computer Science
  GPA: 4.0/4.0

- **B.S. in Computer Engineering,** *LUMS, Pakistan*   **2005**
  Major GPA: 4.0/4.0
  Cumulative GPA: 3.96/4.0

LITIGATION CONSULTING

- **Hogan v. Amazon, Inc.**   **2024**
  Counsel: Wexler Boley & Elgersma LLP
  Client: Wexler Boley & Elgersma LLP
  Court: U.S. District Court, Northern District of Illinois
  Case: 21 C 3169

  - Violation of Illinois biometric information privacy act (BIPA) by facial recognition software
  - Submitted reports

- **McDaniel v. Meta Platforms, Inc.**   **2024**
  Counsel: Bursor & Fisher, P.A.
  Client: Bursor & Fisher, P.A.
  Court: Superior Court of the State of California
  Case: 21-CV-383231

  - Violation of California Consumer Privacy Act (CCPA)
  - Submitted reports

- **Visual Supply Company Consumer Privacy Litigation.**   **2023**
  Counsel: Labaton Sucharow LLP
  Client: Labaton Sucharow LLP
  Court: JAMS Alternate Dispute Resolution
  Case: 1220073248

2

- Violation of Illinois biometric information privacy act (BIPA) by facial recognition software
- Submitted declarations

- **Correct Transmission v. Nokia Corporation**   **2023**
  Counsel: Alston & Bird
  Client: Nokia Corporation
  Court: U.S. District Court, Eastern District of Texas
  Case: 2:22-cv-00343

  - Patent infringement of systems and methods for network transmission and packet fragmentation

- **Collision v. Nokia Corporation**   **2023**
  Counsel: Mckool Smith
  Client: Nokia Corporation
  Court: U.S. District Court, Eastern District of Texas
  Case: 2:21-cv-00327

  - Patent infringement of systems and methods for network transmission and packet fragmentation

- **Ocado Innovation, Ltd. v. Autostore System, Inc.**   **2022**
  Counsel: Sullivan & Cromwell LLP
  Client: Ocado Innovation, Ltd.
  Court: U.S. District Court, District of New Hamshire
  Case: 1:21-00041

  - Patent infringement of automated storage and retrieval system

- **Carl Zeiss X-Ray, Inc. v. Sigray, Inc.**   **2022**
  Counsel: Fish & Richardson P.C.
  Client: Carl Zeiss X-Ray, Inc.
  Court: U.S. District Court, Northern District of California
  Case: 21-cv-01129-EJD

  - Trade secret misappropriation of X-Ray microscopy software

- **Clearview AI, Inc. Consumer Privacy Litigation.**   **2022**
  Counsel: Loevy & Loevy
  Client: Loevy & Loevy
  Court: U.S. District Court, Northern District of Illinois
  Case: 1:21-cv-00135

  - Violation of Illinois biometric information privacy act (BIPA) by facial recognition software
  - Submitted declarations

- **Jane Doe et al., v. Apple, Inc.**   **2022**
  Counsel: Schlichter Bogard & Denton
  Client: Schlichter Bogard & Denton
  Court: U.S. District Court, Southern District of Illinois

3

Case: 3:20-CV-421-NJR

- Violation of Illinois biometric information privacy act (BIPA) by facial recognition software
- Submitted declarations and reports

- **Causam Enterprises, Inc. v. Resideo Technologies, Inc., Itron, Inc.**   **2022**
  Counsel: Alston & Bird
  Client: Resideo Technologies, Inc., Itron, Inc.
  Court: U.S. International Trade Commission
  Case: 337-TA-1277

  - Patent infringement of smart thermostats load control switches and components
  - Submitted expert reports
  - Provided testimony

- **ViaTech Technologies v. Adobe Inc.**   **2021**
  Counsel: Bunsow De Mory LLP
  Client: Bunsow De Mory LLP
  Court: U.S. District Court, District of Massachusetts
  Case: 1:19-cv-11177

  - Patent infringement of DRM technology

- **IP Bridge v. Nokia Corporation**   **2021**
  Counsel: Alston & Bird
  Client: Nokia Corporation
  Court: U.S. District Court, Eastern District of Texas
  Case: 2:21-cv-00215-JRG

  - Patent infringement of systems and methods for radio transmission and reception, downlink channel control, and transmission over shared channel
  -
- **Daedalus Blue v. Microsoft Corporation**   **2021**
  Counsel: BDIP Law
  Client: Daedalus Blue
  Court: U.S. District Court, Western District of Texas
  Case: 6:20-cv-1152

  - Patent infringement of systems and methods for data replication, on demand hosting, scalable virtual machines, and cloud computing environments

- **Daedalus Blue v. MicroStrategy Inc.**   **2021**
  Counsel: BDIP Law
  Client: Daedalus Blue
  Court: U.S. District Court, Eastern District of Virginia
  Case: 1:20-cv-01326

  - Patent infringement of systems and methods for aggregate data processing

- **IPCom v. At&t, Sprint, Verizon, Nokia Corporation**   **2021**
  Counsel: Alston & Bird
  Client: Nokia Corporation
  Court: U.S. District Court, Eastern District of Texas
  Case: 2:20-cv-321, 2:20-cv-322, 2:20-cv-323

  - Patent infringement of systems and methods of transmitting messages in a telecommunication network

- **Firtiva Corporation v. Funimation Global Group, LLC.,**   **2021**
  Counsel: Saul, Ewing, Arnstein, & Lehr
  Client: Firtiva Corporation
  Court: U.S. District Court, Eastern District of Texas
  Case: 2:21-cv-111-JRG-RSP

  - Patent infringement of systems and methods of combining embedded information and content and in electronic transmission
  - Submitted expert reports
  - Provided testimony

- **Universal Electronics, Inc. v. Roku,**   **2021**
  Counsel: Alston & Bird
  Client: Universal Electronics, Inc.
  Court: U.S. International Trade Commission
  Case: 337-TA-1200

  - Patent infringement of televisions, remote controls, and components
  - Submitted expert reports

- **Roku, Inc. v. Universal Electronics, Inc.,**   **2021**
  Counsel: Alston & Bird
  Client: Universal Electronics, Inc.
  Court: U.S. International Trade Commission
  Case: 337-TA-1263

  - Patent infringement of televisions, remote controls, and components thereof
  - Submitted expert reports
  - Provided testimony

- **Vance, et al. v. Amazon.com, Inc.,**   **2021**
  Counsel: Lynch Carpenter LLP and Loevy & Loevy
  Client: Lynch Carpenter LLP and Loevy & Loevy
  Court: U.S. District Court, Western District of Washington
  Case: 2:20-cv-01084

  - Violation of Illinois biometric information privacy act (BIPA) by facial recognition software
  - Submitted declarations

- Provided testimony

- **Vance, et al. v. Microsoft Corporation,**   **2021**
  Counsel: Lynch Carpenter LLP and Loevy & Loevy
  Client: Lynch Carpenter LLP and Loevy & Loevy
  Court: U.S. District Court, Western District of Washington
  Case: 2:20-cv-01082

  - Violation of Illinois biometric information privacy act (BIPA) by facial recognition software
  - Submitted declarations
  - Provided testimony

- **Zellmer v. Facebook, Inc.**   **2021**
  Counsel: Carey Rodriguez Milian, LLP
  Client: Carey Rodriguez Milian, LLP
  Court: U.S. District Court, Northern District of California
  Case: 18-cv-01881-JD

  - Violation of Illinois biometric information privacy act (BIPA) by facial recognition software
  - Submitted expert reports

- **ViaTech Technologies v. Microsoft Corporation**   **2020**
  Counsel: Bunsow De Mory LLP
  Client: Bunsow De Mory LLP
  Court: U.S. District Court, District of Delaware
  Case: 17-570-RGA

  - Patent infringement of DRM technology

- **Packet Intelligence, LLC. v. Nokia Corporation**   **2020**
  Counsel: Alston & Bird
  Client: Nokia Corporation
  Court: U.S. District Court, Eastern District of Texas
  Case: 2:18-cv-382

  - Patent infringement of communication protocols and methods

- **DZ Reserve, et. al. v. Facebook, Inc.**   **2019**
  Counsel: Cohen Milstein Sellers & Toll, PLLC
  Client: Cohen Milstein Sellers & Toll, PLLC
  Court: U.S. District Court, Northern District of California
  Case: 3:18-cv-04978-JD

  - Analyzed source code related to advertisement related statistics
  - Submitted declarations and expert report
  - Provided testimony

- **Polaris PowerLED Technologies, LLC. v. Vizio, Inc.**   **2019**
  - Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
  - Client: Vizio, Inc.
  - Court: U.S. District Court, Central District of California
  - Case: 8:18-cv-01571-JVS (DFMx)

  - Patent infringement of screen brightness control with ambient light

- **Neodron v. Samsung, Microsoft, Amazon, Lenovo, Motorola, Dell, and HP**   **2019**
  - Counsel: Russ August & Kabat
  - Client: Neodron
  - Court: U.S. International Trade Commission
  - Case: Inv. No. 337-TA-1162

  - Patent infringement of capacitive touch screens

- **Autel Robotics, LLC. v. DJI Technology, Ltd.**   **2019**
  - Counsel: Steptoe and Johnson, LLP
  - Client: Autel Robotics, LLC
  - Court: U.S. International Trade Commission
  - Case: Inv. No. 337-TA-1133

  - Analyzed software source code for autonomous aircrafts
  - Submitted expert report

- **Blackberry v. Facebook, Snap**   **2018**
  - Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
  - Client: Blackberry
  - Court: U.S. District Court, Central District of California
  - Case: 2:18-cv-01844 GW(KSx)

  - Patent infringement of advertisement and messaging platforms

- **Broadcom Corp. v. Toyota, Panasonic, Denso Ten, Renesas**   **2018**
  - Counsel: Steptoe and Johnson
  - Client: Broadcom Corp.
  - Court: U.S. International Trade Commission
  - Case: Inv. No. 337-TA-1119

  - Patent infringement of video decoding and graphics systems
  - Lead source code reviewer, managed a team of 5 code reviewers to review a large body of source code across multiple products and vendors

- **Neptune Subsea v. Nokia Solutions & Networks**   **2018**
  - Counsel: Alston & Bird
  - Client: Nokia Solutions & Networks
  - Court: U.S. International Trade Commission

7

Case: Inv. No. 337-TA-1098

- Patent infringement of optical communication systems

- **Broadcom Corp. v. LG, MediaTek, Funai Corp, Sigma Designs, Vizio, Inc.**   **2017**
  Counsel: Steptoe and Johnson
  Client: Broadcom Corp.
  Court: U.S. International Trade Commission
  Case: Inv. No. 337-TA-1047

  - Patent infringement of graphics processing and video decoding systems

- **Home Semiconductors v. Samsung Electronics**   **2018**
  Counsel: Techknowledge Law Group
  Client: Home Semiconductors
  Court: U.S. District Court, District of Delaware
  Case: Civil Action 13-2033-RGA

  - Patent infringement of memory hardware
  - Submitted declarations

- **Implicit LLC v. Sonos, Inc.**   **2018**
  Counsel: Singer Bea LLP
  Client: Implicit LLC
  Court: U.S. District Court, District of Delaware
  Case: Civil Action 17-258-LPS-CJB

  - Patent infringement of audio synchronization and multi-speaker audio systems
  - Submitted declarations
  - Provided testimony

- **Video Gaming Technologies, Inc. v. Castle Hill Studios, LLC, et al**   **2018**
  Counsel: Saul Ewing Arnstein & Lehr LLP
  Client: Castle Hill Studios
  Court: U.S. District Court, Northern District of Oklahoma
  Case: Civil Action 17-cv-454-GKF-JF

  - Trade secret misappropriation of gaming software

- **Implicit LLC v. Palo Alto Networks**   **2017**
  Counsel: Singer Bea LLP
  Client: Implicit LLC
  Court: U.S. District Court, Eastern District of Texas
  Case: Civil Action 6:17-cv-00182-JRG

  - Patent infringement of firewall and network data processing technology
  - Submitted declarations

- **WH Administrators, Inc. v. Corepex Technologies, Inc.**   **2017**
  - Counsel: Berenzweig Leonard, LLP
  - Client: WH Administrators, Inc.
  - Court: U.S. Circuit Court, Eastern District of Virginia
  - Case: Civil Action 1:17-cv-00026

  - Software quality, originality, and copyright infringement
  - Submitted expert reports
  - Provided testimony

- **Corepex Technologies, Inc. v. WH Administrators, Inc.**   **2017**
  - Counsel: Mitchell Silberberg & Knupp
  - Client: WH Administrators, Inc.
  - Court: U.S. District Court, Eastern District of Virginia
  - Case: Civil Action 1:17-cv-00026-LMB-MSN

  - Software quality, originality, and copyright infringement
  - Submitted expert reports
  - Provided testimony

- **Nokia Solutions & Networks v. Huawei Technologies**   **2017**
  - Counsel: Alston & Bird
  - Client: Nokia Solutions & Networks
  - Court: U.S. District Court, Eastern District of Texas
  - Case: 2:16-cv-00753-JRG-RSP

  - Patent infringement of LTE communication protocols and methods
  - Submitted declarations

- **Facebook Biometric Information Privacy Litigation**   **2017**
  - Counsel: Robbins Geller Rudman & Dowd
  - Client: Robbins Geller Rudman & Dowd
  - Court: U.S. District Court, Northern District of California
  - Case: Class Action 3:15-CV-03747-JD

  - Violation of Illinois biometric information privacy act (BIPA) by facial recognition software
  - Submitted expert reports
  - Provided testimony

- **Alexander Yershov v. Gannett Satellite Information Network**   **2017**
  - Counsel: ZwillGen PLLC
  - Client: Gannett Satellite Information Network
  - Court: U.S. District Court, District of Massachusetts
  - Case: Civil Action 1:14-CV-13112-FDS

  - Violation of user privacy by mobile application

9

- **Financial Information Technologies v. Mark Lopez**   **2017**
  Counsel: Rocke McLean Sbar
  Client: Mark Lopez
  Court: U.S. District Court, M.D. Florida, Tampa Division
  Case: Civil Action 15-CA-008938

  - Trade secret misappropriation of database systems

- **Walmart-Stores, Inc. v. Cuker Interactive, LLC**   **2017**
  Counsel: Kutak Rock LLP
  Client: Walmart-Stores, Inc.
  Court: U.S. District Court, Western District of Arkansas
  Case: Civil Action 5:14-CV-5262

  - Copyright infringement of online shopping software

- **Papst Licensing v. Apple, LG, ZTE, Samsung, Lenovo, Motorola, Huawei**   **2016**
  Counsel: DiNovo Price Ellwanger
  Client: Papst Licensing
  Court: U.S. District Court, Eastern District of Texas
  Case: Civil Action No. 6:15-cv-1095

  - Patent infringement of audio/video capture and encoding

- **CSS v. Christopher Herrington, Gene Yoho and Compiled Technologies**   **2016**
  Counsel: Robinson & McElwee
  Client: Christopher Herrington, Gene Yoho and Compiled Technologies
  Court: U.S. District Court, Southern District of West Virginia, Charleston Division
  Case: Civil Action 2:16-CV-01762

  - Copyright infringement and trade secret misappropriation of document management software

RESEARCH

- **Research Assistant**   **2007 – 2011**
  University of Wisconsin, Madison
  - Investigated various structural and functional aspects of the cortical hierarchy
  - Developed processing models and algorithms inspired by biological cortical columns
  - Implemented biologically inspired computational models that are inherently tolerant to transient and permanent hardware faults and errors
  - Introduced the concept of a Neuromorphic Instruction Set Architecture (NISA) to address the semantic challenges introduced by the contemporary neuromorphic architectures
  - Collaborated with researchers from Electrical Engineering, Neuroscience, and Computer Science

- **Research Assistant**   **2006 – 2007**
  University of Wisconsin, Madison

- Worked on designing a Ternary Content Addressable Memory (TCAM) based functional unit to improve the performance of search and recognition (SR) applications.
- Proposed ISA for optimizing the S/R process using the proposed TCAM functional unit
- Implemented several SR applications using the TCAM ISA extensions
- Developed a detailed functional simulator to run the SR applications using the TCAM ISA extensions and investigated the performance benefits of using TCAM functional unit

- **Research Assistant**   **2005 – 2006**
  University of Wisconsin, Madison
  - Developed a software system to control features of a laser-scanning and micro-beam microscopes
  - Designed analog and digital circuits that ensure safety of laser and micro-beam microscopes
  - Interfaced fire wire camera for image acquisition from the microscopes to observe specimens

- **Research Assistant**   **2003 – 2005**
  Lahore Univ. of Management Sciences, Pakistan
  - Developed an Ethernet system for controlling and monitoring electrical appliances
  - Developed hardware for multi-channel data acquisition using computer's joystick port and implemented a software interface to control the hardware and acquire data on a UNIX based system

TEACHING

- **Lead Instructor**   **2009 – 2011**
  PEOPLE Program, University of Wisconsin, Madison
  - Structured, designed, and taught advanced mathematics courses to underrepresented and underprivileged high school students
  - Designed problem sets and assignments to promote outside classroom learning
  - Taught calculus, trigonometry, and algebra

- **Teaching Assistant**   **2008 – 2009**
  University of Wisconsin, Madison
  - Assisted in designing and teaching an introductory freshman level course in computer engineering with an emphasis to promote students interest in engineering
  - Designed and graded problem sets, exams, homework, and assignments
  - Organized regular discussion sessions with students

- **Teaching Assistant**   **2008 – 2009**
  Lahore University of Management Sciences, Pakistan
  - Assisted in designing and teaching courses in the areas of circuit design, computer architecture, and signal and image processing.
  - Designed and graded assignments, projects, exams, and homework
  - Assisted in teaching a graduate level image processing course during senior year

TECHNICAL EXPERTISE

- **Fields**

11

Artificial Intelligence, Deep Learning, Computer Networks, Operating Systems, Computer Architecture, Hardware Design, Object Recognition and Pattern Classification, Image, Audio, and Video Processing, Mobile Applications, Sensor Fusion, "Always-On" Sensing

- **Software Development**
  C/C++, Java, JavaScript, Perl, Python, PHP, Matlab, HTML, Android, Embedded C

- **Hardware Development**
  Verilog HDL design, pre/post synthesis validation, FPGA prototyping

PATENTS

- **Reconfigurable event driven hardware using reservoir computing for monitoring an electronic sensor and waking a processor,** US-9541982-B2, 2016
  - The invention describes a hardware architecture consisting of spiking neural network of ultralow power processing of sensory data in real-time.

- **Systems and methods for analyzing a sensory stream using reservoir computing,** US-20170083081-A1, 2016
  - This invention describes an efficient hardware that utilizes reservoir computing to process sensory data.

- **Neural Sensor Hub System,** US-20160335534-A1, 2015
  - This invention describes an efficient spiking neural network implementation for low memory and low compute microcontrollers along with the infrastructure for training and configuring the network for recognizing complex motion and audio events.

- **Efficient and scalable neural systems for calculating network connectivity for neural algorithms in an event-driven way to reduce storage of data relating to connectivity,** US-20160098629-A1, 2014
  - This invention describes an efficient model for managing and storing connectivity patterns between neurons of a complex neural network implemented in software or as a hardware substrate.

- **Learn-by-example systems and methods,** US-20150254575-A1, 2014
  - This invention describes an web based infrastructure that enables training a neural network to detect complex spatio-temporal events and deploying the trained neural network configuration on a IoT device.

CONFERENCE PUBLICATIONS

1. Andrew Nere, Atif Hashmi, Mikko Lipasti, Giulio Tonini, **Bridging the Semantic Gap: Emulating Biological Neuronal Behaviors with Simple Digital Neurons**, International Symposium on High Performance Computer Architecture, Shenzhen, China, Feb 2013

2. Atif Hashmi, Mikko Lipasti, et. al., **BenchNN: On the Broad Potential Application Scope of Hardware Neural Network Accelerators, International Symposium on Workload Characterization**, San Diego, CA, Nov 2012

12

3. Atif Hashmi, Hugues Berry, Olivier Temam, and Mikko H. Lipasti, **Automatic Abstraction and Fault Tolerance in Cortical Microarchitectures**, International Symposium on Computer Architecture, San Jose, CA, June 2011

4. Atif Hashmi, Andrew Nere, and Mikko H. Lipasti, **Learning through Spatially Localized and Temporally Correlated Spontaneous Activations**, International Conference on Cognitive and Neural Systems, Boston, MA, May 2011

5. Andrew Nere, Atif Hashmi, and Mikko H. Lipasti, **Profiling Heterogeneous Multi-GPU Systems to Accelerate Cortically Inspired Learning Algorithms**, International Parallel and Distributed Processing Symposium, Anchorage, AL, May 2011

6. Atif Hashmi, Andrew Nere, James Thomas, and Mikko H. Lipasti, **A Case for Neuromorphic Instruction Set Architectures**, International Conference on Architectural Support for Programming Languages and Operating Systems, Newport Beach, CA, March 2011

7. Atif Hashmi and Mikko Lipasti, **Discovering Cortical Algorithms**, International Conference on Neural Computation, Valencia, Spain, October 2010

8. Atif Hashmi and Mikko Lipasti, **Cortical Columns: Building Blocks for Intelligent Systems**, IEEE Symposium on Computational Intelligence for Multimedia Signal and Vision Processing, Nashville, TN, March 2009

9. Atif Hashmi and Mikko Lipasti, **Accelerating Search and Recognition with a TCAM Functional Unit**, International Conference on Computer Design, Lake Tahoe, NV, October, 2008

10. Atif Hashmi, Haroon Malik, Aman Pervaiz, and Mohammad Younas, **Cost Effective and Efficient Approach to Control and Monitor Area Network (CMAN)**, International Conference on Microelectronics, Tunis, Tunisia, December, 2004

11. Atif Hashmi and Mohammad Akmal Butt, **Multi-channel Data Acquisition for Implementation of Real Time Signal Processing Algorithms**, IEEE International Multi-topic Conference, Lahore, Pakistan, 2004

JOURNAL PUBLICATIONS

1. Atif Hashmi, Andrew Nere, and Giulio Tononi, **Sleep-dependent synaptic down-selection (II): single-neuron level benefits for matching, selectivity, and specificity**, Frontiers in Neurology, volume 4, DOI: 10.3389/fneur.2013.00148, 2013

2. Andrew Nere, Atif Hashmi, Chiara Cirelli, and Giulio Tononi, **Sleep-dependent synaptic down-selection (I): modeling the benefits of sleep on memory consolidation and integration**, Frontiers in Neurology, volume 4, DOI: 10.3389/fneur.2013.00143, 2013

3. Andrew Nere, Sean Franey, Atif Hashmi, and Mikko Lipasti, **Simulating Cortical Networks on Heterogeneous Multi-GPU Systems**, Journal of Parallel and Distributed Computing, volume 73, issue 7, pages 953-971, 2012

4. Atif Hashmi and Mikko Lipasti, **A Cortically Inspired Learning Model**, Studies in Computational Intelligence, volume 399, pages 373-388, 2012

TECHNICAL/INVITED TALKS

13

1. **Integrating multiple modalities via reentrant hierarchical attractor networks**, The Brain Corporation, San Diego, CA, June 2011

2. **Addressing the Semantic Gap in Neuromorphic Systems**, Asilomar Microcomputer Workshop, Pacific Grove, CA, April 2011

3. **A case of abstract yet accurate cortical models**, University of Minnesota, Minneapolis, MN, Feb 2011

4. **Automatic Abstraction and Fault Tolerance in Cortical Microarchitectures**, International Symposium on Computer Architecture, San Jose, CA, June 2011

5. **Learning through Spatially Localized and Temporally Correlated Spontaneous Activations**, International Conference on Cognitive and Neural Systems, Boston, MA, May 2011

6. **Cortical Architectures: From Learning to Creativity, Google Technical Talk**, Madison, WI, December 2010

7. **Discovering Cortical Algorithms, International Conference on Neural Computation (ICNC)**, Valencia, Spain, October 2010

8. **Cortical Microarchitectures: Computing by Abstractions**, UW - Computer Architecture Affiliates, Madison, WI, October 2010

9. **Discovering Cortical Algorithms**, International Conference on Cognitive and Neural Systems (ICCNS), Boston, MA, May 2010

10. **Leveraging Progress in Neurobiology for Computing Systems**, Workshop on New Directions in Computer Architecture/International Symposium on Microarchitecture, New York, NY, December 2009

11. **PHARM Brain v 2.0: Lateral Communication Paths and Feedback**, UW - Computer Architecture Affiliates, Madison, WI, December 2009

12. **Cortical Columns: Building Blocks for Intelligent Systems**, Symposium on Computational Intelligence for Multimedia Signal and Vision Processing (CIMSVP), Nashville, TN, March 2009

13. **Accelerating Search and Recognition with a TCAM Functional Unit**, International Conference on Computer Design (ICCD), Lake Tahoe, NV, October 2008

HONORS AND AWARDS

- **Expert due-diligence panelist/reviewer for National Science Foundation (NSF)**
  - Evaluate proposal submitted to NSF in the areas of sensor based systems and machine learning

- **Principal Investigator for National Science Foundation SBIR Phase I and II Awards,** 2014
  - This is granted by NSF to fund cutting-edge research performed by a small business

- **National Science Foundation Innovation Corps Award,** 2012
  - This is granted by NSF to entrepreneurs performing market research related to a startup venture

14

- **Valedictorian Wisconsin Entrepreneurial Bootcamp,** 2012
  - This awards is granted by the University of Wisconsin – School of Business to promising entrepreneurs

- **Best paper award, IEEE International Parallel & Distributed Processing,** 2011
  - This award is granted to the best paper published in a peer-reviewed conference

- **Recipient of NMF Gold Medal, B.S. class of 2005**
- **Recipient of Excellence Gold Medal for the best overall student, B.S. class of 2005**
- **Recipient of Dean's Honor Shield for graduating with distinction, B.S. class of 2005**
- **Class Valedictorian, B.S. class of 2005**
- **Recipient of LUMS Merit Scholarship for exceptional academic performance**
  - Granted for exceptional academic and extra-curricular accomplishments

- **Best project award, IEEE International Electronics Design Contest for Students (IEDCS), 2004**
  - Granted to the best project and paper published in a peer-reviewed conference

- **Recipient of Award of Academic Excellence, 2003**
- **Recipient of President's Gold Medal, 2003**
  - Awarded by the President of Pakistan for securing 1st position in the annual district level exam

15

EXHIBIT B

1271 Avenue of the Americas
New York, New York 10020-1401
Tel: +1.212.906.1200 Fax: +1.212.751.4864
www.lw.com

LATHAM&WATKINS LLP

FIRM / AFFILIATE OFFICES

Austin	Milan
Beijing	Munich
Boston	New York
Brussels	Orange County
Century City	Paris
Chicago	Riyadh
Dubai	San Diego
Düsseldorf	San Francisco
Frankfurt	Seoul
Hamburg	Silicon Valley
Hong Kong	Singapore
Houston	Tel Aviv
London	Tokyo
Los Angeles	Washington, D.C.
Madrid	

August 16, 2024
VIA EMAIL

Jonathan M. Rotter
jrotter@glancylaw.com
Glancy Prongay & Murray LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150

Re: *Lau v. Gen Digital*, Case No. 3:22-cv-08981-RFL

Dear Jonathan,

We write as a follow-up to our recent conversations, in which we have discussed why the transmissions of cookie data you have proffered as the basis for Plaintiffs' claims in fact have benign explanations and do not lend any genuine support to those claims. In this letter, we detail the explanation for the transmissions at issue—readily discoverable from publicly available information—and provide definitive evidence that the cookie data included in the headers of these transmissions is (a) not requested by Avast Online Security & Privacy ("AOSP") and (b) not used after the transmissions are received by Avast servers. We also explain why you do not need any further discovery in order to confirm these conclusions, including the discovery you have recently requested via email and in supplemental interrogatories and document requests.

We hope that the information herein persuades you to voluntarily dismiss this case, as it confirms what we have said from the outset of this matter—that you have no basis to allege that Avast somehow uses cookies to provide AOSP user browsing data to third parties for advertising purposes. If you choose not to voluntarily dismiss the complaint, however, and instead continue litigating despite now being on clear notice that your factual contentions lack evidentiary support, we warn you that you will be in continuing violation of your Rule 11 obligations, and that we fully intend to seek sanctions at an appropriate time.

A.   **Plaintiffs' Theory: Cookie Header Data in Traffic Sent to Avast Is
(a) Embedded by AOSP and (b) Used by Avast for Third-Party Advertising**

Plaintiffs' surviving claims rest on the factual premise that AOSP somehow "intercepts" and "uses" cookies to share AOSP user browsing data with third-party advertisers. As the Amended Complaint states:

AOSP uses approximately forty-five third-party advertising cookies designed to transmit the intercepted, collected, and stored data on its servers to numerous third-party advertising partners, including Google, MS Advertising, and Adalyser.

LATHAM&WATKINS LLP

> Through these cookies, private data intercepted, collected, and stored by AOSP …
> was and is provided for use by these third parties for targeted advertising, to the
> financial benefit of Defendants.[1]

The Amended Complaint itself does not explain how exactly AOSP is supposed to "use" third-party advertising cookies to "provide" data collected through AOSP to third parties, or what basis Plaintiffs supposedly had for making for this key allegation.

In response to Gen Digital's contention interrogatories, however, Plaintiffs subsequently provided the putative basis for the allegation. Specifically, Plaintiffs asserted: "When a device that has the AOSP plugin installed on it ('AOSP Client Device') visits a webpage, AOSP intercepts the request to the website and sends it to Avast's servers, along with third-party cookies that Avast installed on the AOSP Client Device browser."[2] As evidence for this assertion, Plaintiffs provided printouts of the data that they observed being sent from their browsers to urlite.ff.avast.com—the Avast service to which AOSP sends URLs that users visit, for analysis ("URLite Service"). This data, Plaintiffs pointed out, contains an HTTP cookie header. An example is as follows[3]:

---

[1] Am. Compl. ¶ 80, Dkt. 47.

[2] Plaintiff Halim's Supp. Responses and Objections to Defendants' First Interrogatories, at 11.

[3] *Id.* at 14.

LATHAM&WATKINS LLP

According to Plaintiffs, the cookies contained in these headers (the "Subject Cookies") "are installed on an AOSP user's device when the user is guided to or visits Avast's webpage."[4] Plaintiffs stated that "Avast uses the Subject Cookies to transmit data to third-party advertising partners in at least the following ways: (1) embedding the Subject Cookies in AOSP's transmissions of user data from users' devices to Avast's servers; and (2) transmitting the user data associated with embedded cookies that Avast received from AOSP to third-party advertising partners' servers through server-to-server communication."[5] Plaintiffs implicitly acknowledged they have no visibility into what Avast does through "server-to-server communication" with third parties, stating that their claim that Avast transmits user browsing and cookie data to third-party advertising partners is based on "information and belief."[6]

In short, Plaintiffs have explained the basis for their case as follows:

(1) Plaintiffs see a cookie header in HTTP traffic that their browser sends to the URLite Service.

(2) Plaintiffs assume that *Avast* is the one that "embed[s]" this cookie data in the transmissions.

(3) Plaintiffs speculate—on "information and belief"—that, once the transmissions hit the URLite Service, Avast pairs URL data collected from AOSP with the cookie data in the HTTP header, and transmits the combined data to third-party advertisers.

B.   Plaintiffs' Theory Is Demonstrably Wrong

The assumption and speculation that underlie Plaintiffs' theory of the case (specifically premises (2) and (3) above) are simply wrong—demonstrably so. The cookie header Plaintiffs have observed in traffic sent to the URLite Service is not embedded by Avast; it is sent by Plaintiffs' own browsers, without any request from AOSP for the data. Nor does Avast do anything with this cookie data once the transmission reaches the URLite Service. These points can be confirmed through a simple, targeted review of certain aspects of the AOSP and URLite Service code.

1.   The Cookie Header Is Added by Plaintiffs' Browsers, Not Avast

First, as to why a cookie header appears in traffic sent from Plaintiffs' browsers to the URLite Service, it has nothing to do with AOSP and everything to do with how browsers and cookies operate within the HTTP protocol. Every cookie has a domain attribute that can be set for it, which defines the domain with which a browser will share the cookie. Whenever the

---

[4] *Id.* at 9.

[5] *Id.* at 10-11.

[6] *Id.* at 11 ("On information and belief, based on the nature of the advertising, tracking, and data-sharing cookies from third parties installed on AOSP users' devices, Plaintiff further states that from the AOSP user's browser, the data is transmitted to an AOSP server, and from the AOSP server the data is transmitted to a third-party server.")

LATHAM&WATKINS LLP

browser communicates with any server on that domain, the browser will *automatically* append any cookies associated with that domain to the communication, by including them within the HTTP header for the communication.[7] For example, if a cookie is installed on a browser and has a domain attribute of "example.com," then any time the browser communicates with a server on the example.com domain, the browser will automatically append the data for that cookie in the HTTP cookie header of the message. Likewise, if the browser communicates with a server on a subdomain of the domain associated with the cookie (e.g., "forum.example.domain"), the browser will automatically append the cookie data to messages sent to that subdomain as well.[8]

The domain attribute of the Subject Cookies is set to "avast.com." These cookies are installed on a user's browser when they visit the avast.com website and are used by Avast in connection with the operation of the website (as well as various associated subdomains, e.g., buy.avast.com, my.avast.com, and support.avast.com).[9] The only reason you are seeing these cookies appended to traffic sent to the URLite Service is that the URLite Service also resides on an avast.com subdomain—urlite.ff.**avast.com**—even though it is not part of the Avast website and does not use cookies. AOSP is a browser extension and as such communicates through a user's browser. Again, based on the way the HTTP protocol works, when a browser communicates with a server on a particular domain, it will automatically check for any cookies stored on the browser that are associated to that domain, and include those cookies in the communication header. Thus, when AOSP sends URL data to the URLite Service, the browser sees that the message is directed to a server on the avast.com domain, checks for any cookies associated to that domain, finds the Subject Cookies, and appends them to the message. In short, the *browser* "embeds" the cookies in the traffic—not AOSP.

Beyond looking at publicly available primers on how cookies work, Plaintiffs can also confirm this by looking at the AOSP client-side code. That code is not minified[10] and can be decompiled and reviewed using publicly available tools, as you apparently have done already, judging from your references to particular lines of AOSP code in your latest set of document

---

[7] See*, e.g.*, Javascript.Info, *Cookies*, https://javascript.info/cookie ("Cookies are usually set by a web server using the response Set-Cookie HTTP header. Then, the browser automatically adds them to (almost) every request to the same domain using the Cookie HTTP header."); Mozilla Developer Network, *Using HTTP Cookies*, https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies ("When a new request is made, the browser usually sends previously stored cookies for the current domain back to the server within a Cookie HTTP header.").

[8] *See, e.g.*, Mozilla Developer Network, *Using HTTP Cookies*, https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies ("The Domain attribute specifies which server can receive a cookie. If specified, cookies are available on the specified server *and its subdomains*."); HTTP.dev, *Set-Cookie*, https://http.dev/set-cookie ("The domain attribute refers to the host that the cookie will be sent to. … [S]ubdomains are always included when a domain is specified.").

[9] If a user opts out of cookies through the cookie banner on the Avast.com website, the cookies remain on the user's device, but they are not used by Avast for advertising purposes.

[10] Minifying code refers to removing unnecessary characters to reduce the size of the code files, which has the effect of making it less readable by humans.

LATHAM&WATKINS LLP

requests.[11] If you search the AOSP code for references to headers, you will find that the only references to HTTP headers of any kind are in the background.js file, where there are references to the "content-type" and "x-requested-with" headers.[12] There is no reference of any kind to the cookie header. The absence of any such reference definitively disproves any notion that AOSP is requesting the cookie header or otherwise "embedding" it in traffic sent to the URLite Service.

2.   AOSP Does Not Use the Data in the Cookie Header

Not only does AOSP not request the data in the cookie header you are seeing, but Avast does not do anything with it when it is received by the URLite Service. This can again be demonstrated through a targeted search of the relevant code. In order for the URLite Service to do anything with data in the cookie header, the URLite Service would need to collect that header from the communication, using the "headers.get" method.[13] The code for the URLite Service contains no "get" request for—or any other reference to—the HTTP cookie header. Attached hereto as Exhibit A are the results of searches we have conducted across all versions of the URLite Service code from 2021 to 2024 for references to *any* type of HTTP header. The only HTTP headers that appear in the results are:

- Content-Length
- Content-Type
- User-Agent
- X-Forwarded-For

The absence of any reference to the cookie header in the code definitively disproves any notion that the URLite Service retrieves or uses the data in the HTTP cookie header in any way—let alone for purposes of pairing it with URL data and sharing the combined data with third-party advertisers.

In sum, the cookie data that you have observed being transmitted to the URLite Service is extraneous data that is appended to the transmissions by the users' browsers, as mere happenstance from the fact that the transmissions are being sent to a server on the avast.com domain. The cookie data is simply ignored by the URLite Service, as it has nothing to do with the functioning of AOSP.

---

[11] *See* Plaintiffs' Second Set of Requests for Production dated Aug. 5, 2024, at Request Nos. 69-71 and 74-77.

[12] These references can be found in the current version of the Chrome version of the extension at lines 12489 and 25482 of the background.js file, or in the current version of the Edge version of the extension by opening the background.js file and searching for "headers."

[13] *See, e.g.*, Mozilla Developer Network, *Headers:get()*, https://developer.mozilla.org/en-US/docs/Web/API/Headers/get ("The get() method of the Headers interface returns a byte string of all the values of a header within a Headers object with a given name. If the requested header doesn't exist in the Headers object, it returns null.")

LATHAM&WATKINSLLP

        C.   **Plaintiffs Do Not Need Further Discovery to Confirm That Avast Does Not Do What They Claim**

       The foregoing facts and attached evidence provide all the information needed to confirm that your claims have no evidentiary basis. We are willing to provide a sworn declaration attesting to the above facts and authenticating the attached evidence if it would be helpful. We are also willing to consider any other narrowly focused discovery requests you wish to make relating to details of the above.

       However, we will continue to oppose broadsweeping or irrelevant requests for information of the sort you have made to date. In particular, in your email dated August 1, 2024, you informally asked Gen Digital to produce:

- "Server-side and database-side source code during the relevant period for servers and databases involved in AOSP's operations, including but not limited to the server-side application code, and including all changes made;"

- "Server-side and database-side source code during the relevant period for servers and databases involved in receiving, processing, and/or storing any data transmitted by the AOSP client, including but not limited to the server-side application code, and including all changes made;"

- "For June 5-10, 2022, January 11-20, 2023, and February 9-11, 2023:

  o Server configurations, including the CORS policy, for www.avast.com/

  o Server configurations for all servers involved in AOSP's operations, including but not limited to the urlite.ff.avast.com subdomain servers;

  o Database schema for all databases involved in AOSP's operations, including but not limited to the urlite.ff.avast.com subdomain databases;

  o A representative data dump for each of the servers and databases involved in AOSP's operations;

  o A log file for each of the servers and databases involved in AOSP's operations."

       None of the foregoing is necessary for you to verify that Avast does not use HTTP cookie headers appended to traffic sent to the URLite Service. In particular, you do not need to review the entire code base that runs on the URLite Service (including all changes made to the code base over several years' time), which would be unduly burdensome for Gen Digital to produce, particularly given the highly confidential nature of the AOSP code base and the cumbersome conditions that would have to be put in place in making it available to you. You only need to review, at most, portions of the code base involving HTTP header data, which we are providing herewith. Nor do you need "server configurations" for the avast.com website or the URLite

LATHAM&WATKINSLLP

Service, or "log files" for severs or databases involved in AOSP's operations—none of which have any ostensible relevance to whether AOSP or the URLite Service utilizes cookie data.

As to your requests for "database schema" and "a representative data dump" for all servers or databases involved in AOSP's operations, it is unclear what you mean. To the extent you are seeking a description or sample of the data that is stored in the course of operating AOSP, the only data that would be relevant to your claims would be that relating to the use of cookies, which does not exist. Nonetheless, to facilitate our discussions, we are providing the following materials:

- Attached as Exhibit B is documentation from Avast's internal Github repository explaining the data stored by the URLite Service. Note that the URLite Service is used by multiple client applications, including but not limited to AOSP, and the data it stores varies by application in certain respects.

- Specifically, the GitHub page explains that the URLite Service stores a "hit feed," consisting of visits to URLs already classified by Avast as malicious. The URLite Service can store an individual identifier as part of this hit feed if the client application provides it, but AOSP does not provide any such identifiers to the URLite Service, let alone any identifiers based on cookies. This can be seen from Exhibit C attached hereto, which contains a sample of the hit feed data collected from AOSP. As it reflects, the "client_info" field is "null" for all of the entries. (Please note that all of the URLs in this exhibit are malicious and should not be visited.)

- The GitHub page also explains that the URLite Service can send "clickstream" data, consisting of all URLs visited by users, to another system for further processing. Clickstream data is in fact collected from AOSP and is used as part of the process for detecting novel malicious links or other malicious attributes. As noted in the GitHub page, however, clickstream data does not include any individual identifiers. It only includes the client platform (Android, Windows, iOS, etc.), product (i.e., AOSP), and country location derived from IP address.

These additional materials further confirm that Plaintiffs' cookie allegations have no basis in fact.

You have also recently promulgated a formal set of supplemental interrogatories and document requests, despite indicating earlier that you were willing to pursue confirmatory discovery on an informal basis. We will provide our objections to these requests in due course, but none of them are relevant to the factual question on which the case turns—namely, whether Avast combines URL data with cookie data and shares it with third-party advertisers. Some of the supplemental requests appear designed to fish for entirely new theories of liability—such as requests concerning information about "cross-domain data sharing," or the "privacy implications" of including a "credentials parameter" in an "HTTP fetch call function" in an older version of AOSP. We will adamantly object to these and any other discovery requests that seek to expand the scope of the case, or that otherwise are not focused on the narrow (and erroneous) factual theory underlying Plaintiffs' surviving claims.

LATHAM&WATKINS LLP

D.   Continuing to Pursue Your Claims Despite Knowing They Lack an Evidentiary Basis Is Sanctionable Under Rule 11

In light of the information provided herein, we hope that, consistent with your ethical obligations, you will agree to voluntarily dismiss this case. If you do not, we warn you again that we will seek sanctions for your pursuit of claims that you never adequately investigated in the first place and that, in any event, you now clearly know lack evidentiary support.

Rule 11(b) provides that, by submitting a pleading, an attorney certifies that "to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances … the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery." Fed. R. Civ. P. 11(b). From the outset, the cookie-related allegations in the Amended Complaint have had no evidentiary support. Indeed, you have conceded that the only basis for making the allegations is that you observed cookie headers being included in traffic sent to the URLite Service from Plaintiffs' browsers. Had you conducted a reasonable inquiry into *why* such headers were appearing, you would have consulted basic information about the HTTP protocol and how cookies and browsers work, readily available from public sources, which would have revealed that browsers automatically append cookies associated to a specified domain whenever the browser communicates with any server on that domain. Further, you would have also reviewed the client-side source code for AOSP—which, again, is publicly accessible—for any references to the cookie header, which would have revealed that AOSP does not make any request for this information. You evidently did not conduct any such inquiry, but instead leapt to the conclusion that *AOSP* was "embedding" the cookie headers you were observing. That is not the sort of reasonable investigation that Rule 11 requires. *See Lake v. Hobbs*, 643 F. Supp. 3d 989, 1009 (D. Ariz. 2022) (imposing Rule 11 sanctions upon finding that "any objectively reasonable investigation of this case would have led to publicly available and widely circulated information contradicting Plaintiffs' allegations and undercutting their claims"); *PageMelding, Inc. v. ESPN, Inc*., 2012 WL 1534844, at *2 (N.D. Cal. Apr. 30, 2012) (finding plaintiff failed to comply with Rule 11 obligations when the complaint rested on a pleading approach of "shoot first and ask questions later"); *see also Zaldivar v. City of L.A.,* 780 F.2d 823, 831 (9th Cir. 1986)) ("[T]he conclusion drawn from [plaintiffs'] research undertaken must itself be defensible. Extended research alone will not save a claim that is without legal or factual merit from the penalty of sanctions.").

And of course, as to the most critical allegation of the Amended Complaint—that Avast somehow *uses* these cookies to send user browsing data to third-party advertisers—you have conceded that the allegation is based on mere "information and belief." That is simply a polite way of saying that the allegation is based on nothing but your own speculation and surmise, and that you never had—and still do not have—any evidentiary basis for it. *See Martinez v. City of West Sacramento*, 2021 WL 2227830, *6 (E.D. Cal. Jun. 2, 2021) ("Simply affixing the term 'on information and belief' to [an allegation] does not grant Plaintiffs free license to assert a multitude of specific facts without any evidentiary basis."); *Delphix Corp. v. Actifo, Inc*., 2014 WL 4628490, at *2 n.3 (N.D. Cal. Mar. 19, 2014) ("Despite the common appearance of that phrase in practice, it is not a recognized pleading device under the rules" but rather "creates [an] inference that plaintiff likely lacks knowledge of underlying facts to support the assertion, and is

LATHAM&WATKINS LLP

instead engaging in speculation to an undue degree.").[14]

In any event, based on the information we have provided you since the filing of the Amended Complaint, including the facts and evidence provided in this letter, you are now clearly on notice that your claims have no evidentiary basis. To persist nonetheless in pursuing the claims in the Amended Complaint would separately violate Rule 11. The duty imposed by Rule 11 is a continuing one: Not only does the rule "require litigants to 'stop-and-think' before initially making legal or factual contentions," but "[i]t also …. emphasizes the duty of candor by subjecting litigants to potential sanctions for insisting upon a position after it is no longer tenable." Fed. R. Civ. P. 11(b)–(c) (advisory committee's note to 1993 amendment). Many courts have recognized this ongoing duty. *See, e.g.*, *Smith v. Ricks*, 31 F.3d 1478, 1488 (9th Cir. 1994) ("Counsel can no longer avoid the sting of Rule 11 sanctions by operating under the guise of a pure heart and empty head."); *SG Blocks, Inc. v. Hola Cmty. Partners*, 2021 WL 2714596, at *2 n.5 (C.D. Cal. July 1, 2021) (holding in light of 1993 amendment that "it is clear that Rule 11 does impose a continuing duty"); *Avedisian v. Mercedes-Benz USA, LLC*, 2014 WL 47466, at *4 (C.D. Cal. Jan. 2, 2014) ("Rule 11 also subjects litigants to sanctions for insisting upon a position after it is no longer tenable."); *Nguyen v. Simpson Strong-Tie Co., Inc.*, 2020 WL 5232564, at *5 (N.D. Cal. Sept. 2, 2020) ("Plaintiffs' refusal to withdraw or meaningfully amend these allegations, which were core to its FAC, was a violation of Rule 11 [as amended]."); *Martinez*, 2021 WL 2227830, at *3, 15 (E.D. Cal. June 2, 2021) ("[T]he Court finds imposing a monetary sanction is necessary to deter [plaintiff] from further refusing to withdraw or correct contentions after a potential violation is called to his attention or insisting upon a position after it is no longer tenable, as such litigation tactics serve only to waste precious public resources.").

Given that you are now undeniably aware that your position in this case "is no longer tenable," Rule 11 prohibits you from "insisting upon it." We therefore ask you to voluntarily dismiss this case as promptly as possible. We do not wish to bring a sanctions motion against you and your clients, but we will if you persist in pursuing the baseless allegations in your Amended Complaint and generating unnecessary litigation costs for Gen Digital.

Sincerely,

Serrin Turner

---

[14] Nor did the Amended Complaint identify this as an allegation for which Plaintiffs lacked evidentiary support and only expected to obtain it later, as Rule 11(b) requires if that was Plaintiffs' intention. *See* Fed. R. Civ. P. 11(b)(3) (providing that submission of a pleading certifies that all factual contentions have evidentiary support "or, *if specifically so identified*, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery"); *see also Martinez v. City of W. Sacramento*, 2021 WL 2227830, *6 (E.D. Cal. June 2, 2021) ("[I]f a party does not have evidentiary support for his allegation at the time of filing but 'will likely have evidentiary support after a reasonable opportunity for further investigation or discovery,' Rule 11 expressly requires that the allegation be identified as such.").